UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

SIMA KESLER Plaintiff(s) v. T-MOBILE USA, INC.; DOES 1 through 10, inclusive, Defendant(s)	Civil Action No. Jury Trial Demanded

Sima Kesler ("Plaintiff"), on behalf of herself individually, alleges as follows against T-Mobile, Inc. ("T-Mobile") and others:

I. INTRODUCTION

1. It is generally recognized that mishandling of customers' accounts, including (but not limited to) allowing unauthorized access to customers' information, leads to identity theft and related consumer harm.

2. These types of events, however, have occurred on numerous occasions at T-Mobile – one of the nation's largest wireless carriers – and are now a matter of routine.

3. In this sense, the present action is (unfortunately) very typical – it arises out of T-Mobile's failure to safeguard Plaintiff's highly sensitive personal and financial information that resulted in the theft of Plaintiff's cryptocurrency.[1]

4. As a result of the misconduct alleged herein, Plaintiff lost in excess of $20,000.00 in cryptocurrency (as valued at the time of the loss) in an account takeover scheme (commonly

[1] Cryptocurrency (also known as "crypto") is a virtual asset designed as a medium of monetary exchange that is verified by an encrypted digital ledger called "blockchain." It is decentralized and is often traded through various "exchanges," such as Coinbase, Inc. ("Coinbase").

known as “SIM-swapping”) that would not have occurred but for the abject violations of federal and state laws at issue.

II. THE PARTIES

5. Plaintiff is an adult individual citizen of the Commonwealth of Pennsylvania, who resides in Philadelphia County.

6. T-Mobile is a corporation formed under the laws of the State of Delaware, with headquarters and principal place of business in Bellevue, Washington, that serves as the American operating “arm” of T-Mobile International AG & Co., a corporate entity based in Germany.

7. Plaintiff is unaware of the names and capacities of those defendants sued as DOES 1 through 10, but will seek leave to amend this complaint once their identities become known to Plaintiff. Upon information and belief, Plaintiff alleges that at all relevant times, each defendant, including the DOE defendants 1 through 10, was the officer, director, employee, agent, representative, alter ego, or co-conspirator of each of the other defendants, and in engaging in the conduct alleged herein was in the course and scope of and in furtherance of such a relationship.

8. Unless otherwise specified, Plaintiff will refer to all defendants collectively as “Defendant” and each allegation pertains to each Defendant.

9. At all times material hereto, Defendant acted and/or failed to act in person and/or through duly authorized agents, servants, workmen, and/or employees, acting within the scope and course of their authority and/or employment for and/or on behalf of Defendant.

III. JURISDICTION AND VENUE

10. This Honorable Court has jurisdiction pursuant to 28 U.S.C. § 1331, 28 U.S.C. § 1332, 28 U.S.C. § 1367, and 47 U.S.C. § 207.

11. The Eastern District of Pennsylvania is the proper venue for this litigation, because:

a. Plaintiff is a resident of the Eastern District of Pennsylvania;

b. The wrongful conduct was directed to and was undertaken within the territory of the Eastern District of Pennsylvania; and

c. T-Mobile conducts a substantial portion of its business in the Eastern District of Pennsylvania.

IV. STATEMENT OF CLAIMS

A. GENERAL BACKGROUND

12. As one of the nation's largest wireless carriers, T-Mobile's operations must comply with various federal and state statutes, including (but not limited to) the Federal Communications Act ("FCA"), 47 U.S.C. § 222.

13. The FCA obligates T-Mobile to protect the "confidential proprietary information of [its] customers" and "customer proprietary network information" (commonly referred to as "CPI" and "CPNI," respectively). See 47 U.S.C. § 222(a), (c).

14. The Federal Communications Commission ("FCC") has promulgated rules to implement Section 222 of the FCA "to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI." 1998 CPNI Order, 13 FCC Rcd. at 8195 ¶193; see also 47 C.F.R. § 64.2001 et seq. ("CPNI Rules").

15. The CPNI Rules limit disclosure and use of CPNI without customer approval to certain limited circumstances (such as cooperation with law enforcement), none of which are applicable to the facts here. See 47 C.F.R. § 64.2005.

16. The CPNI Rules also require carriers to implement safeguards to protect customers' CPNI. See 47 C.F.R. § 64.2009(b), (d), and (e).

17. These safeguards include: (a) training personnel "as to when they are and are not

authorized to use CPNI[;]" (b) establishing "a supervisory review process regarding carrier compliance with the rules[;]" and (c) filing annual compliance certificates with the FCC. Id.

18. The CPNI Rules further require carriers to implement measures to prevent the disclosure of CPNI to unauthorized individuals. For example, "carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." See 47 C.F.R. § 64.2010(a).

19. T-Mobile regularly holds itself out to the general public as a secure and reliable custodian of customer data, including confidential financial and personal information.

20. T-Mobile maintains that it uses a variety of "administrative, technical, contractual, and physical safeguards" to protect customers' data.[2]

21. As an example, T-Mobile explicitly states that "when you contact us by phone or visit us in our stores, we have procedures in place to make sure that **only** the primary account holder or authorized users have access."[3]

22. Upon information and belief, T-Mobile's sales and marketing materials make similar representations regarding T-Mobile's alleged implementation of various safeguards to protect its customers' private information.

23. Despite these assurances and other similar statements, T-Mobile failed to provide reasonable and appropriate security to prevent unauthorized access to customers' accounts.

24. For instance, upon information and belief, under the inadequate procedures implemented by T-Mobile, unauthorized persons, including T-Mobile's own officers, agents, and

[2] https://www.t-mobile.com/privacy-center/our-practices/privacy-policy, last visited on June 2, 2021.

[3] Id. (emphasis supplied).

employees, acting without customer permission, can authenticate, access, and make changes to customers' information.

25. T-Mobile failed to disclose or made deceptive statements designed to cover up for the fact that its security procedures can and do fall short of its expressed and implied representations and promises.

26. Such failures leading to unauthorized access of customers' information were entirely foreseeable by T-Mobile.

B. "SIM-SWAPPING" SCAM

27. As T-Mobile is aware, various forms of account takeover fraud have been widely reported in the press, by government regulators, including the Federal Trade Commission ("FTC") and the FCC, as well as in academic publications.

28. These illegal schemes involve criminals and fraudsters gaining access to or "hijacking" customer wireless accounts, which often include sensitive personal and financial information, to induce third parties to conduct transactions with individuals they believe to be legitimate or known to them.

29. One of the most damaging and pervasive forms of account takeover fraud is known as "SIM-swapping" (or "SIM-jacking"), whereby a criminal third-party convinces a wireless carrier like T-Mobile to transfer access to one of its legitimate customer's cellular phone number from the legitimate customer's registered "subscriber identity module" card (or "SIM card") – a small portable chip that houses identification information connecting an account to the wireless carrier's network[4] – to a SIM card controlled by the criminal third-party.

[4] A SIM card is a small, removable chip that allows a cell phone to communicate with the wireless carrier and to know which subscriber is associated with that phone. The SIM card associated with a wireless phone can be changed, allowing customers to move their wireless number from one cell

30. The wireless carrier, however, must effectuate the SIM card reassignment and, therefore, "SIM-swapping" is not an isolated criminal act, as it requires the wireless carrier's active involvement to swap the SIM containing information regarding its customer to an unauthorized person's phone.

31. Indeed, unlike a direct hack of data, where a company like T-Mobile plays a more passive role, "SIM-swaps" are ultimately effectuated by the wireless carrier itself. For instance, in this case, it is T-Mobile that approved and allowed the SIM card change, as well as all of the subsequent telecommunication activity that was used to hack Plaintiff's online accounts and cause the injuries suffered by Plaintiff.

32. Once the third-party has access to the legitimate user's SIM card data, it can then seamlessly impersonate that legitimate wireless customer (e.g., in communicating with others or contacting various vendors).

33. A common target of "SIM-swapping" and account takeover fraud are individuals known, or expected, to hold cryptocurrency, because account information is often contained on users' cellular phones, allowing criminals to transfer the legitimate user's cryptocurrency to an account the criminal controls.[5]

34. "SIM-swapping" is not a new unforeseeable phenomenon but, instead, has been discussed by federal authorities since at least 2016.

35. In June 2016, the FTC's then Chief Technologist, herself a victim of an account

---

phone to another and to continue accessing their carrier network when they switch cell phones.

[5] Indeed, earlier this year, T-Mobile was subject to a lawsuit, where as a result of a "SIM-swap" a cryptocurrency holder lost in excess of $450,000.00. See Cheng v. T-Mobile USA, Inc., Docket No. 1:21-cv-01085-PKC (S.D.N.Y); see also Middleton, et al. v. T-Mobile US, Inc., Docket No. 1:20-cv-03276-NGG-RLM (E.D.N.Y.)(asserting a loss of $8.7 million of cryptocurrency as a result of "SIM-swap" of a T-Mobile account).

takeover scam, recounted her experience and offered advice to wireless carriers to help consumers avoid these takeover attacks, stating:

> The mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking and fraudulent new accounts. In fact, many of them are obligated to comply with the Red Flags Rule, which, among other things, requires them to have a written identity theft prevention program. Carriers should adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions … [M]obile carriers and third-party retailers need to be vigilant in their authentication practices to avoid putting their customers at risk of major financial loss and having email, social network, and other accounts compromised.[6]

36. Attention in the media and by government regulators, however, did not ensure that wireless carriers like T-Mobile took security seriously enough to prevent account takeover accounts and "SIM-swapping" schemes from increasing or, worse, to convince themselves, company-wide, to stop engaging in practices that flouted federal law.

37. An empirical study conducted by researchers at Princeton University and publicized in early 2020 (the results of which were known to T-Mobile prior to publication) "identified weak authentication schemes and flawed policies" at several major wireless carriers in the United States, including T-Mobile.[7]

38. The study further demonstrated that "these flaws enable[d] straightforward SIM

---

[6] Lorrie Cranor, "Your mobile phone account could be hijacked by an identity thief," Tech@FTC (June 7, 2016), available at https://www.ftc.gov/. Mrs. Cranor also detailed her concerns about "SIM-swapping" in her reply comments before the FCC in July 2016. See In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunication Services, WC Docket No. 16-106 (July 6, 2016).

[7] Kevin Lee, et al., "An Empirical Study of Wireless Carrier Authentication for SIM Swaps," Dept. of Comp. Sci. and Ctr. for Info. Tech. Policy, Princeton University (Jan. 10, 2020), pp. 2, 10 (discussing T-Mobile's discontinuation of call log verification based on the study's research in January 2020).

swap attacks," as the researchers succeeded in all ten of their attempts to effectuate a SIM-swap on T-Mobile accounts. Id.

39. This study established a clear vulnerability of T-Mobile's customer authentication process that enabled criminals to easily secure access to the personal information of T-Mobile's customers.

40. Even before the results of the Princeton study were made available to T-Mobile, however, in May 2018, a popular information security blog, "Krebs on Security," detailed several failures by T-Mobile to keep its customers' data secure, including lack of adequate supervision of T-Mobile's employees (one of whom perpetuated an account takeover scheme with knowledge of T-Mobile's vulnerable internal systems) and failing to send legitimate customers notice to their personal e-mail when a "SIM-swap" occurs.[8]

41. The article pointed out that "[T-Mobile] also acknowledged that it does not currently send customers an email to the email address on file when SIM swaps take place. A T-Mobile spokesperson said the company was considering changing the current policy, which sends the customer a text message to alert them about the SIM swap" to the phone number that is now in the criminal third-party's control.[9]

42. As the blog's author concluded with regard to sending a text to a phone number that is already hijacked, "obviously that does not help someone who is the target of a SIM swap."[10]

43. In a 2019 article about "SIM-swapping" that included multiple quotes from T-

[8] Brian Krebs, "T-Mobile Employee Made Unauthorized 'SIM Swap' to Steal Instagram Account," Krebs on Security (May 18, 2018), available at https://krebsonsecurity.com/.

[9] Id.

[10] Id.

Mobile personnel, the New York Times explicitly reported that "[c]riminals have learned how to persuade mobile phone providers **like T-Mobile** and AT&T to switch a phone number to a new device that is under their control."[11]

44. In February of 2020, the FCC issued a "Notice of Apparent Liability for Forfeiture and Admonishment," proposing a penalty of $91,630,000.00 against T-Mobile for misuse of CPNI, where Commissioner Geoffrey Starks explained:

> Going forward, Americans must be able to place trust in their wireless carriers. . . .[T]hese carriers know that the services they offer create risks for users: unauthorized location tracking, **SIM hijacking**, and billing scams to name just [a] few. **Carriers must take responsibility for those people they allow into their operations**.[12]

45. Despite the massive amounts of media, governmental, and academic focus on the issue of "SIM-swapping" and the internal vulnerabilities of wireless carrier systems, T-Mobile has been unable or unwilling to institute the practices, procedures, and safeguards necessary to protect its customers' data from account takeover and "SIM-swap" attacks.

46. Most troubling, T-Mobile has not improved its safety protocols even though it knows from numerous incidents that some of its own employees actively cooperate with hackers in "SIM-swap" frauds by allowing direct access to customer information and/or by ignoring or overriding T-Mobile security procedures.

47. The prevalence of "SIM-swap" fraud and T-Mobile's knowledge of such fraud, including (but not limited to) with active participation of its own employees, demonstrate that what

---

[11] Nathaniel Popper, "Hackers Hit Twitter C.E.O. in a 'SIM swap.' You're at Risk, Too," New York Times (September 5, 2019)(emphasis supplied).

[12] In the Matter of T-Mobile USA, Inc., File No. EB-TCD-18-00027702 (February 28, 2020)(emphasis supplied).

happened with Plaintiff's account was neither an isolated incident nor an unforeseeable event.

48. As a regulated wireless carrier, T-Mobile has a well-established duty – one which it freely acknowledges on its corporate website – to protect the security and privacy of CPI and CPNI from unauthorized access and T-Mobile is obligated to certify its compliance with this mandate to the FCC every year.[13]

49. In light of the above, at the time of the events at issue in the present case, T-Mobile was keenly aware of its obligations, as well as multiple weaknesses in its internal processes and procedures to authenticate legitimate customers.

50. Yet, T-Mobile failed to prevent the "SIM-swap" in this case, causing Plaintiff to lose in excess of $20,000.00 in cryptocurrency (at the time of the loss) that today is valued in excess of $65,000.00.

C. THE "SIM-SWAP" OF PLAINTIFF'S ACCOUNT

51. In May of 2020, Plaintiff was a 71-years old female, who used T-Mobile as her personal mobile telecommunications carrier.

52. At that time, Plaintiff was holding cryptocurrency for personal use on Coinbase – a digital currency wallet and online platform to transfer and store digital currency – using Coinbase's application ("mobile app") on Plaintiff's mobile phone, as well as her computer.

53. Plaintiff entrusted her sensitive private information, including (but not limited to) regarding her cryptocurrency holdings, to T-Mobile and relied on T-Mobile's assurances of and and its compliance with applicable laws, including (but not limited to) the FCA.

54. At approximately 8:00 p.m., on Saturday, May 2, 2020, Plaintiff realized that her

[13] See, e.g., https://www.t-mobile.com/privacy-center/education-and-resources/cpni, last visited on June 2, 2021.

mobile phone was disconnected from service.

55. Plaintiff initially believed that this was a temporary glitch in coverage and attempted to restart the mobile phone.

56. Plaintiff became concerned, however, when, after numerous attempts, the interruption in service continued and she was still unable to make calls, send text messages, or access any of her mobile apps.

57. Plaintiff checked her Coinbase account from her computer and did not notice any suspicious or inappropriate activity.

58. Unable to resolve the service issue herself, at 8:32 p.m., on May 2, 2020, Plaintiff contacted T-Mobile's online support chat and reported that she lost all service to her mobile device.

59. While in the chat with T-Mobile's personnel, at 9:12 p.m., on May 2, 2020, Plaintiff suddenly received an e-mail from Coinbase that her password for the application was reset.

60. Plaintiff became suspicious of the sudden loss in cellular service and concerned with T-Mobile's apparent inability to resolve the issue.

61. She immediately attempted to log into her Coinbase account from her desktop computer, but her access was now denied.

62. Although Plaintiff's online chat with T-Mobile's personnel lasted until approximately 11:00 p.m., at no point in time did anyone from T-Mobile explain to Plaintiff why her service was disconnected or advise Plaintiff that she may be a victim of a "SIM-swap."

63. Subsequently, Plaintiff learned that, at 7:53 p.m., on May 2, 2020, unknown individual(s) visited a T-Mobile store, where T-Mobile personnel allowed and provided them unauthorized access to Plaintiff's SIM data, including CPI and CPNI, that said data was then transferred (or "ported") to another electronic device, and used to access Plaintiff's information

and telecommunications service.

64. In other words, Plaintiff was, in fact, a victim of a "SIM-swap" that was effectuated and facilitated by T-Mobile and its employees.

65. Plaintiff did not authorize T-Mobile or anyone else to use, disclose, or access her CPI and CPNI that was maintained by T-Mobile.

66. To the contrary, Plaintiff had an objectively-reasonable expectation and a fundamental right to conduct her personal activities without observation, intrusion, or interference.

67. Therefore, any use, disclosure, or access to Plaintiff's account or CPI and CPNI on May 2, 2020 was unauthorized and unlawful.

68. Later, when Plaintiff was able to re-gain access to her Coinbase account, she discovered that, while T-Mobile personnel kept Plaintiff in the online chat, in a series of coordinated transactions – immediately after Plaintiff's Coinbase password was re-set – that took place at 9:13 p.m. and 9:14 p.m., on May 2, 2020 (i.e., more than an hour after Plaintiff's account was compromised and more than forty minutes after Plaintiff alerted T-Mobile of the unusual service interruption), Plaintiff's Coinbase account was depleted of virtually all cryptocurrency and its proceeds transferred to an unknown third-party account.

69. Hence, it was not just T-Mobile's act of providing the unknown hacker(s) with access to Plaintiff's account without adhering to T-Mobile's security protocols, but also T-Mobile's failure to timely and properly diagnose the cause of Plaintiff's service interruption, as well as to notify Plaintiff, that allowed the cryptocurrency theft to occur.

70. Unfortunately, by the time Plaintiff was able to regain access to her account on Coinbase, her digital wallet was depleted of virtually all cryptocurrency that Plaintiff owned.

71. Plaintiff alerted local law enforcement authorities of this development and, to the

best of Plaintiff's knowledge, the investigation into the identify of the third parties who gained access to Plaintiff's SIM data from T-Mobile is ongoing.

72. Upon information and belief, T-Mobile, despite a legal obligation to do so, abjectly failed in its duty to safeguard its customers' personal and financial information by providing unauthorized access to Plaintiff's CPI and CPNI.

73. Upon information and belief, T-Mobile failed to implement and/or maintain security policies and procedures sufficient to protect the unauthorized access to Plaintiff's CPI and CPNI.

74. Upon information and belief, T-Mobile failed to properly train and supervise its employees to prevent the unauthorized access to Plaintiff's CPI and CPNI.

75. Upon information and belief, T-Mobile could have reasonably foreseen the consequences of failing in its duty to implement, maintain, and execute sufficient security policies and practices to protect the unauthorized access to customer data, including that of Plaintiff.

76. Upon information and belief, T-Mobile's systems, policies, and procedures allow its officers, agents, and employees to exceed the authorized access to customers' accounts without permission or justification.

77. T-Mobile's actions and inaction demonstrate a reckless disregard for the rights of its customers and those with whom its customers deal (i.e., other foreseeable victims).

78. T-Mobile's actions and inaction also demonstrate a reckless disregard for its obligations, responsibilities, and duties under the law.

79. The damage suffered by Plaintiff is directly related to the wrongful conduct of allowing the unauthorized access to Plaintiff's wireless account.

80. Indeed, but for T-Mobile's reckless disregard of its obligations, Plaintiff would not

have been damaged.

C. CAUSES OF ACTION

COUNT I
Violation of Section 222 of the FCA
Against T-Mobile

81. Plaintiff hereby incorporates all facts and allegations of this document by reference, as if fully set forth at length herein.

82. T-Mobile is a "common carrier" or a "telecommunications carrier" engaged in interstate commerce by wire for the purpose of furnishing communication services within the meaning of Section 201(a) of the FCA. See 47 U.S.C. § 201(a).

83. As a "common carrier," T-Mobile is subject to the substantive requirements of Sections 201 through 222 of the FCA. See 47 U.S.C. §§ 201-222.

84. Section 206 of the FCA, entitled "Carriers' liability for damages," provides:

> In case any common carrier shall do, or cause or permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney's fee, to be fixed by the court in every case of recovery, which attorney's fee shall be taxed and collected as part of the costs in the case.[14]

85. Section 207 of the FCA, entitled "Recovery of damages," further provides:

> Any person claiming to be damaged by any common carrier subject to the provisions of this chapter may either make complaint to the [FCC] as hereinafter provided for, or may bring suit for the recovery of the damages for which such common carrier may be liable under the provisions of this chapter, in any district court of the United States of competent jurisdiction; but such person shall not have the

[14] 47 U.S.C. § 206.

right to pursue both such remedies.[15]

86. Section 222(a) of the FCA explicitly requires that a telecommunications carrier protect, *inter alia*, its customers' CPI. See 47 U.S.C. § 222(a).

87. Additionally, Section 222(c) of the FCA explicitly requires that telecommunications carrier protect, *inter alia*, its customers' CPNI. See 47 U.S.C. § 222(c).

88. According to the CPNI Rules:

> Safeguarding CPNI. Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.
>
> * * *
>
> In-store access to CPNI. A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.[16]

89. T-Mobile violated its duties under Section 222 of the FCA by failing to protect Plaintiff's CPI and CPNI by using, disclosing, or permitting access to Plaintiff's CPI and CPNI without the consent, notice, and/or legal authorization of Buchanan as required by the FCA, in that upon information and belief:

a. During an in-store visit, Plaintiff's CPI and CPNI was disclosed to someone other than Plaintiff;

---

[15] 47 U.S.C. § 207.

[16] 47 C.F.R. § 64.2010(a), (d). For purposes of the CPNI Rules, the term "customer" means "[a] person . . . to which the telecommunications carrier is currently providing service," while the term "valid photo ID" means "a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired." 47 C.F.R. § 64.2004(f), (r).

b. During an in-store visit, Plaintiff's CPI and CPNI was disclosed to someone, who was not properly authenticated;

c. During an in-store visit, Plaintiff's CPI and CPNI was disclosed to someone, who did not first present a valid photo ID; and/or

d. During an in-store visit, Plaintiff's CPI and CPNI was disclosed to someone, who did not match any of Plaintiff's account information that T-Mobile was aware of, including (but not limited to) that Plaintiff was a 71-years old female.

90. As alleged herein, T-Mobile failed to protect the confidentiality of Plaintiff's CPI and CPNI when it disclosed Plaintiff's CPNI and CPI to third-parties without Plaintiff's authorization or permission.

91. T-Mobile's conduct, as alleged herein, constitutes a knowing violation of Section 222 of the FCA and the CPNI Rules.

92. T-Mobile is also liable for the acts, omissions, and/or failures, as alleged herein, of its officers, employees, agents, or any other persons acting for or on behalf of T-Mobile.

93. T-Mobile's violations of Section 222 allowed unauthorized parties to impersonate Plaintiff in transactions with others.

94. T-Mobile violated Section 222 by allowing an unauthorized party to access Plaintiff's CPI and CPNI, resulting in, *inter alia*, Plaintiff's loss of cryptocurrency valued in excess of $20,000.00 (at the time of the loss) that today would be worth in excess of $65,000.00.

95. As a direct consequence of T-Mobile's violations of the FCA, Plaintiff has been damaged in an amount of at least $20,000.00.

96. Had T-Mobile not allowed the unauthorized access to Plaintiff's account, Plaintiff

would not have suffered this loss.

97. T-Mobile, by its inadequate procedures, practices, and regulations, engages in practices which, taken together:

a. Fail to provide reasonable, appropriate, and sufficient security to prevent unauthorized access to its customers' wireless accounts;

b. Allow unauthorized persons to be authenticated; and

c. Grant access to sensitive customer account information.

98. In particular, T-Mobile failed to establish and implement reasonable policies, procedures, and safeguards governing the creation, access, and authentication of user credentials to access customers' accounts, creating an unreasonable risk of unauthorized access.

99. As such, in violation of the FCA, T-Mobile has failed to ensure that only authorized persons have access to customer account data and that customers' CPI and CPNI are secure.

100. Among other things, T-Mobile:

a. Failed to establish and enforce rules and procedures sufficient to ensure only authorized persons have access to T-Mobile customer accounts, including that of Plaintiff;

b. Failed to establish appropriate rules, policies, and procedures for the supervision and control of its officers, agents, and employees;

c. Failed to establish and enforce rules and procedures, or provide adequate supervisions or training sufficient to ensure that its employees and agents follow such rules and procedures, to restrict access by unauthorized persons;

d. Failed to establish and enforce rules and procedures to ensure T-Mobile's

employees and agents adhere to the security instructions of customers with regard to accessing customers' accounts, including that of Plaintiff;

e. Failed to adequately safeguard and protect its customers' wireless accounts;

f. Permitted the sharing of and access to user credentials among T-Mobile's agents or employees without a pending request from the customer, reducing the likely detection of and accountability for unauthorized access;

g. Failed to appropriately supervise employees and agents, who granted unauthorized access to customers' accounts, including that of Plaintiff;

h. Failed to adequately train and supervise its employees, officers, and agents to prevent the unauthorized access to customer accounts;

i. Failed to prevent the ability of employees, officers, and agents to access and make changes to customer accounts without specific customer authorization;

j. Allowed "porting out" of cell phone numbers without properly confirming that the request was coming from legitimate customers;

k. Lacked proper monitoring and, therefore, failed to monitor its systems for the presence of unauthorized access in a manner that would allow T-Mobile to detect intrusions, breaches of security, and unauthorized access to customer information;

l. Failed to implement and maintain readily available best practices to safeguard customer information;

m. Failed to timely diagnose and determine the cause of Plaintiff's service interruption;

n. Failed to timely notify Plaintiff of the the cause of Plaintiff's service interruption; and

o. Failed to implement and maintain internal controls to help protect against account takeovers and SIM-swapping by unauthorized persons.

101. The inadequate security measures, policies, and safeguards employed by T-Mobile created an unreasonable risk of unauthorized access to the accounts of its customers, including that of Plaintiff.

102. Upon information and belief, T-Mobile has been long aware of its inadequate security measures, policies, and safeguards and, nevertheless, induced customers into believing that its systems were secure and compliant with applicable law.

103. T-Mobile, despite knowing the risks associated with unauthorized access to customer accounts, failed to utilize reasonable and available methods to prevent or limit such unauthorized access.

104. T-Mobile failed in its duty to protect and safeguard customer information and data pursuant to federal law.

105. Had T-Mobile implemented appropriate and reasonable security measures, Plaintiff would not have been damaged.

106. In sum, T-Mobile's security measures were entirely inadequate to prevent the foreseeable damage caused to Plaintiff.

COUNT II
Negligence
Against T-Mobile and Does 1-10

107. Plaintiff hereby incorporates all facts and allegations of this document by reference, as if fully set forth at length herein.

108. T-Mobile owes a duty of care to its customers to ensure the privacy and confidentiality of CPI and CPNI during its provision of wireless carrier services, as required by both federal and state law.

109. By allowing unauthorized access to the personal and confidential information of legitimate T-Mobile customers, T-Mobile breached its duty of care to its customers and to foreseeable victims, including Plaintiff.

110. By failing to timely and properly diagnose the cause of Plaintiff's service interruption, T-Mobile breached its duty of care to its customers and to foreseeable victims, including Plaintiff.

111. But for the inadequate security protocols, practices, and procedures employed by T-Mobile in protecting customer data, including Plaintiff's private and confidential information, Plaintiff would not have suffered any damage.

112. But for the inadequate protocols, practices, and procedures employed by T-Mobile in diagnosing the causes of customers' service interruptions, T-Mobile breached its duty of care to its customers and to foreseeable victims, including Plaintiff.

113. Moreover, but for T-Mobile's inability to quickly and effectively diagnose and/or determine that Plaintiff's account was compromised by "SIM-swap" – a fact that T-Mobile should have known – Plaintiff would not have suffered any damage.

114. Plaintiff has been damaged in an amount which exceeds $20,000.00.

COUNT III
Negligent Hiring, Retention, and Supervision
Against T-Mobile and Does 1-10

115. Plaintiff hereby incorporates all facts and allegations of this document by reference, as if fully set forth at length herein.

116. At all material times herein, T-Mobile's agents, officers, and employees, including (but not limited to) those directly or indirectly responsible for or involved in allowing unauthorized access to Plaintiff's confidential and proprietary account information, were under T-Mobile's direct supervision and control.

117. Upon information and belief, T-Mobile negligently hired, retained, controlled, trained, and supervised the officers, agents, and employees under its control, and knew or should have known that such officers, agents, and employees could allow unauthorized access to customer accounts, including that of Plaintiff.

118. Upon information and belief, T-Mobile negligently failed to implement systems and procedures necessary to prevent its officers, agents, and employees from allowing unauthorized access to customer accounts, including that of Plaintiff.

119. Upon information and belief, T-Mobile's negligent hiring, retention, control, training, and supervision allowed the unauthorized access to customers' accounts resulting in damage to T-Mobile customers and foreseeable victims in the public at large, including Plaintiff.

120. Given T-Mobile's experience with account takeover and "SIM-swap" attacks (including many that were assisted by the actions of its officers, agents, and/or employees), T-Mobile's failure to exercise reasonable care in screening, supervising, and controlling its officers, agents, and employees was a breach of its duty to its customers, including Plaintiff.

121. T-Mobile's duty to its customers and foreseeable victims to protect its customers' data from unauthorized access is required by federal and state law.

122. It was entirely foreseeable to T-Mobile that unauthorized persons would attempt to gain unauthorized access to T-Mobile customers' data and, despite this, T-Mobile failed to implement sufficient safeguards and procedures to prevent its officers, agents, and employees from

granting such unauthorized access.

123. Upon information and belief, T-Mobile engaged in the acts alleged herein and/or condoned, permitted, authorized, and/or ratified the conduct of its officers, agents, and employees.

124. As a direct consequence of T-Mobile's negligent hiring, retention, control, and supervision of its officers, agents, and employees, who allowed the unauthorized access to Plaintiff's account, Plaintiff was damaged in an amount to be proved at trial that, upon information and belief, exceeds $20,000.00.

COUNT IV
Gross Negligence
Against T-Mobile and Does 1-10

125. Plaintiff hereby incorporates all facts and allegations of this document by reference, as if fully set forth at length herein.

126. T-Mobile, as required by federal and state law, owed Plaintiff a duty to properly handle and safeguard Plaintiff's CPI and CPNI and access to her account.

127. T-Mobile was required to ensure its compliance with federal law and to protect the confidentiality of its customers' account data, including that of Plaintiff.

128. Upon information and belief, T-Mobile willfully disregarded and/or showed reckless indifference to its duties under federal and state law to T-Mobile customers and to foreseeable victims of T-Mobile's wrongful acts.

129. Having superior knowledge of prior account takeover attacks on T-Mobile customers' data and having the ability to employ internal systems, procedures, and safeguards to prevent such attacks, T-Mobile nevertheless failed:

a. to institute appropriate controls to prevent unauthorized access to customers' accounts;

b. utilized authentication systems it knew or should have known were vulnerable to account takeover attacks; and

c. willfully disregarded the best practices of the industry in failing to implement systems to thwart such attacks; and

d. failed to appropriately hire, retain, supervise, train, and control those officers, agents, and employees, who could grant unauthorized access to customer account data.

130. T-Mobile's policies, procedures, and safeguards were completely ineffective and inadequate to prevent the unauthorized access to its customers' data, notwithstanding the requirements of the CFA.

131. T-Mobile's actions as alleged herein, in the face of an abundance of attention by the media and government regulators, evidence a carelessness that can only be characterized as a complete disregard for the rights of its customers and the foreseeable victims of its inadequate data security measures.

132. As a consequence of T-Mobile's gross negligence, Plaintiff has been damaged in an amount to be proved at trial that, upon information and belief, exceeds $20,000.00.

COUNT V
Violation of the Stored Communications Act
Against T-Mobile and Does 1-10

133. Plaintiff hereby incorporates all facts and allegations of this document by reference, as if fully set forth at length herein.

134. Under the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 et seq., "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that

service." 18 U.S.C. § 2702(a)(1).

135. Section 2702(a)(2) of the SCA further states:

> [A] person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; [or] (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing. . . .[17]

136. Although the SCA contains several exceptions to the prohibitions set forth in Sections 2702(a)(1) and (2), none of them are applicable to the circumstances at issue in this case.

137. The SCA creates a private right of action for those "aggrieved by any violation" of its provisions. 18 U.S.C. § 2707(a).

138. The conduct of T-Mobile and Does 1-10, as alleged herein, constitutes a knowing and/or intentional violation of the SCA's Section 2702(a).

139. Plaintiff has been "aggrieved" by the conduct of T-Mobile and Does 1-10, as alleged herein, in that, Plaintiff has lost at least $20,000.00 worth of cryptocurrency.

140. Pursuant to the applicable provisions of the SCA, Plaintiff is entitled to actual and statutory damages, as well as reasonable attorneys' fees and costs. See 18 U.S.C. § 2702(c).

COUNT VI
Violation of the Wiretapping and Electronic Surveillance Control Act
Against T-Mobile and Does 1-10

141. Plaintiff hereby incorporates all facts and allegations of this document by reference,

[17] 18 U.S.C. § 2702(a)(2).

as if fully set forth at length herein.

142. Under Section 5742(a)(1) of the Wiretapping and Electronic Surveillance Control Act ("WESCA"), 18 Pa.C.S. § 5701 et seq.:

> A person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service . . . [o]n behalf of, and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of the service [or s]olely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any such communication for the purpose of providing any services other than storage or computer processing.[18]

143. Under Section 5742(a)(2) of the WESCA:

> A person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service . . . [o]n behalf of, and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of the service [or s]olely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any such communication for the purpose of providing any services other than storage or computer processing.[19]

144. Under Section 5742(a)(3) of the WESCA, "[a] person or entity providing an electronic communication service or remote computing service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to, or customer of, the service." 18 Pa.C.S. § 5742(a)(3).

145. Although WESCA contains several exceptions to the prohibitions set forth in

[18] 18 Pa.C.S. § 5742(a)(1)(i), (ii).

[19] 18 Pa.C.S. § 5742(a)(2)(i), (ii).

Section 5742(a), none of them are applicable to the circumstances at issue in this case. See 18 Pa.C.S. § 5742(b), (c), (c.1).

146. WESCA creates a private right of action for those "aggrieved by any violation" of its provisions. See 18 Pa.C.S. § 5747.

147. The conduct of T-Mobile and Does 1-10, as alleged herein, constitutes a knowing and/or intentional violation of WESCA's Section 5742(a).

148. Plaintiff has been "aggrieved" by the conduct of T-Mobile and Does 1-10, as alleged herein, in that, Plaintiff has lost at least $20,000.00 worth of cryptocurrency.

149. Pursuant to the applicable provisions of WESCA, Plaintiff is entitled to actual and statutory damages, as well as reasonable attorneys' fees and costs. See 18 Pa.C.S. § 5747(c).

COUNT VII
Violation of the Unfair Trade Practices and Consumer Protection Law
Against T-Mobile

150. Plaintiff hereby incorporates all facts and allegations of this document by reference, as if fully set forth at length herein.

151. The Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 P.S. § 201-1 et seq., provides, in pertinent part, that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce . . . are hereby declared unlawful." 73 P.S. § 201-3.

152. Section 201-2(4) of the UTPCPL defines "unfair or deceptive acts or practices" to include the following conduct:

a. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another;

b. Failing to comply with the terms of any written guarantee or warranty given

to the buyer at, prior to, or after a contract for the purchase of goods or services is made; and

c. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding.[20]

153. T-Mobile's acts as alleged herein, including (but not limited to) its sales and marketing representations about its level of data security and confidentiality and the measures T-Mobile employs to keep customers' data secure, induced customers to trade with T-Mobile notwithstanding T-Mobile's knowledge that its security protocols and procedures were inadequate to prevent unauthorized access to customers' CPI and CPNI.

154. Plaintiff justifiably relied on these sales and marketing representations.

155. T-Mobile's actions, as alleged herein, violated federal and state law, particularly those related to the safeguarding of customers' CPI and CPNI and such violations are violations of the above-referenced provisions of the UTPCPL.

156. Given T-Mobile's superior knowledge of its systems, procedures, and practices, coupled with its experience with past breaches of data security (and, specifically, "SIM-swaps") Plaintiff was a foreseeable victim of the violative acts of T-Mobile.

157. By allowing unauthorized access to Plaintiff's confidential and proprietary information, T-Mobile facilitated unauthorized third parties to prey upon innocent victims like Plaintiff.

158. By failing to timely and properly diagnose the cause of Plaintiff's service interruption, T-Mobile facilitated unauthorized third parties to access Plaintiff's confidential and proprietary information and to use said information to steal Plaintiff's property.

[20] See 73 Pa.C.S. § 201-2(4)(vii), (xiv), and (xvii).

159. Had T-Mobile accurately represented the nature of its security measures, or lack thereof, Plaintiff would not have become T-Mobile's customer and would not have been damaged by those who gained unauthorized access to her CPI and CPNI from T-Mobile.

160. Therefore, T-Mobile has violated the above-referenced provisions of 73 Pa.C.S. § 201-2(4).

161. Section 201-9.2(a) of the UTPCPL, authorizes a private cause of action for any person "who purchases or leases goods or services primarily for personal, family or household purposes." 73 P.S. § 201-9.2(a).

162. UTPCPL also authorizes the Court, in its discretion, to award up to three (3) times the actual damages sustained for its violations, as well as attorneys' fees.

163. Plaintiff has suffered and will continue to suffer damages due to the conduct of T-Mobile, as set forth herein.

V. CLAIM FOR RELIEF

WHEREFORE, Plaintiff respectfully prays for:

(a) A Declaration that Defendant has violated the applicable provisions of the FCA, SCA, WESCA, and the UTPCPL;

(b) Actual damages;

(c) Statutory damages;

(d) Treble damages;

(e) Attorneys' fees and costs; and

(f) Such other relief as the Honorable Court shall deem just and appropriate.

VI. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury as to all issues so triable.

Date: June 2, 2021

Respectfully submitted,
KALIKHMAN & RAYZ, LLC

Arkady "Eric" Rayz
1051 County Line Road, Suite "A"
Huntingdon Valley, PA 19006
Telephone: (215) 364-5030
Facsimile: (215) 364-5029
E-mail: erayz@kalraylaw.com

Counsel for Plaintiff